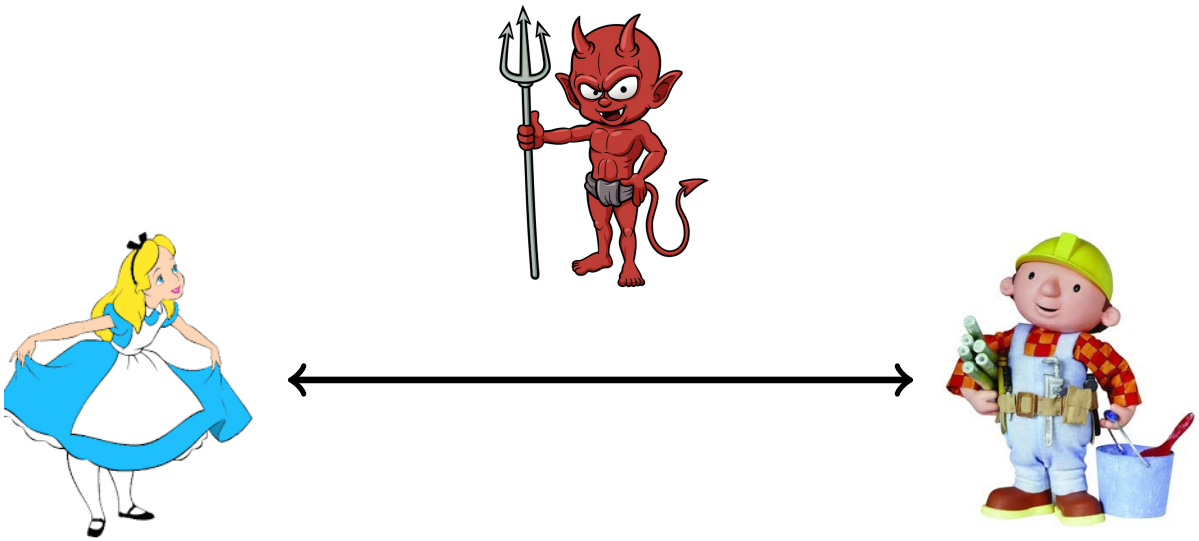
Discrete Mathematics for Symmetric Cryptography

Yann Rotella

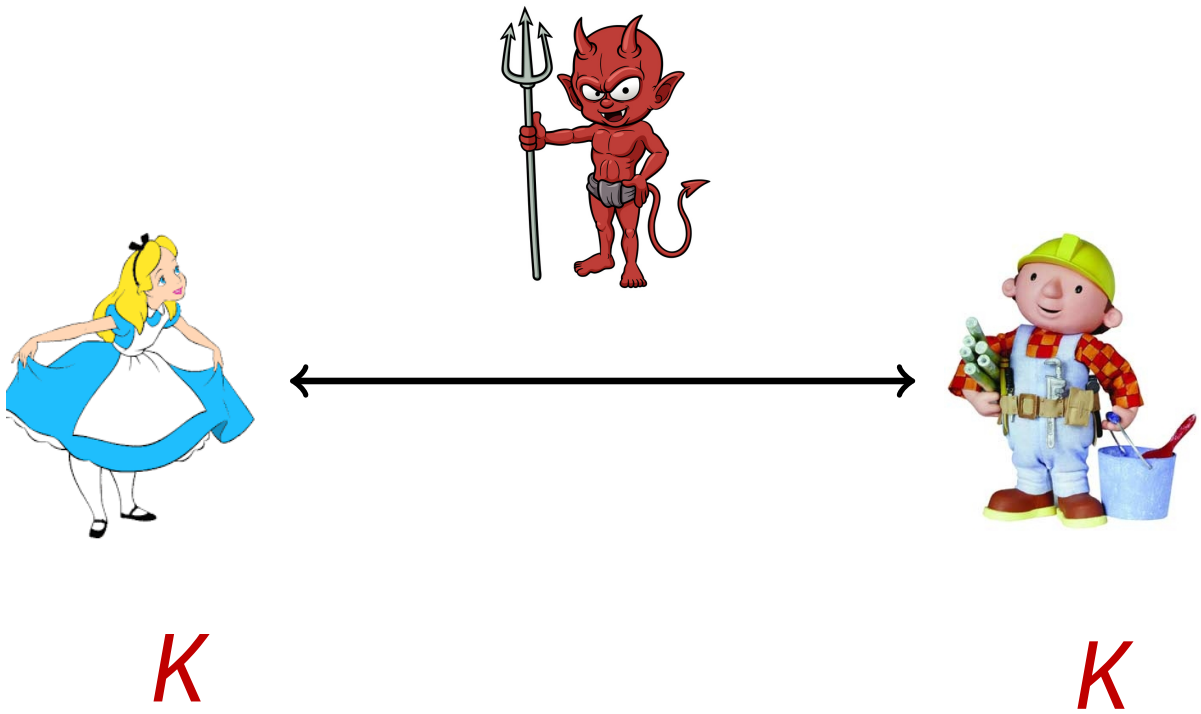
September 19, 2018

Cryptography

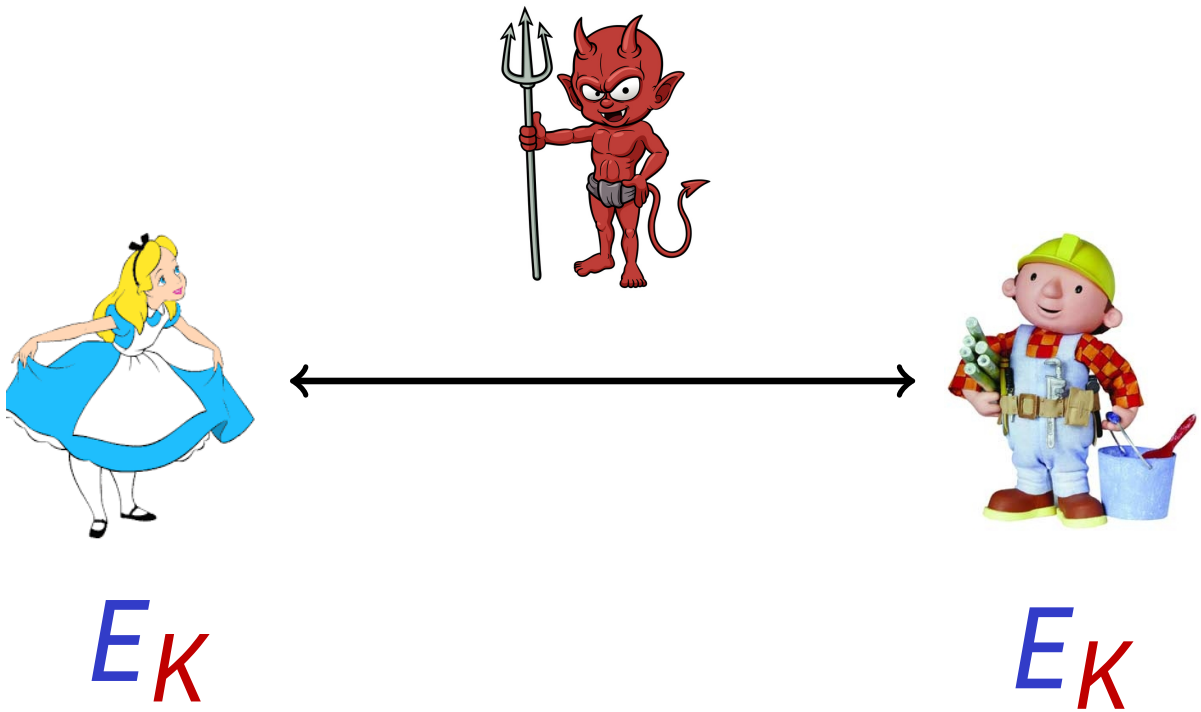


- Authenticity
- Integrity
- Confidentiality

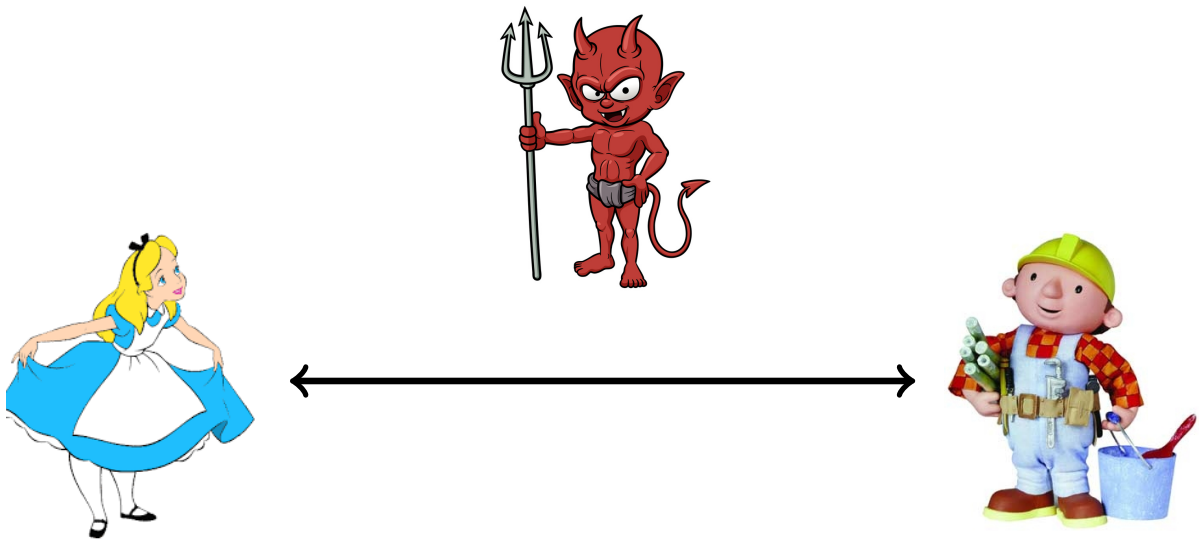
Symmetric Cryptography



Symmetric Cryptography



Symmetric Cryptography



$$c = E_K(m) \qquad m = E_K^{-1}(c)$$

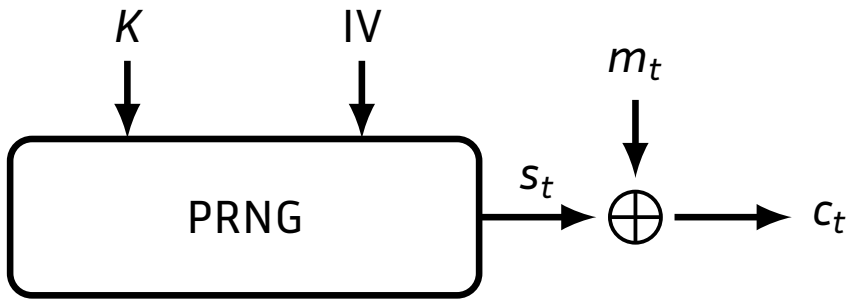
Stream ciphers vs Block ciphers

- Additive stream ciphers

- Block ciphers

Stream ciphers vs Block ciphers

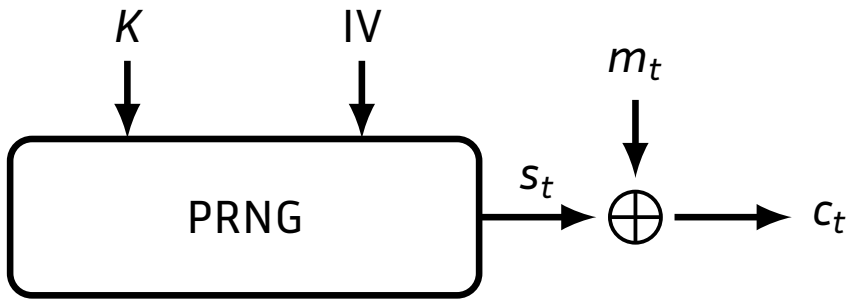
- Additive stream ciphers



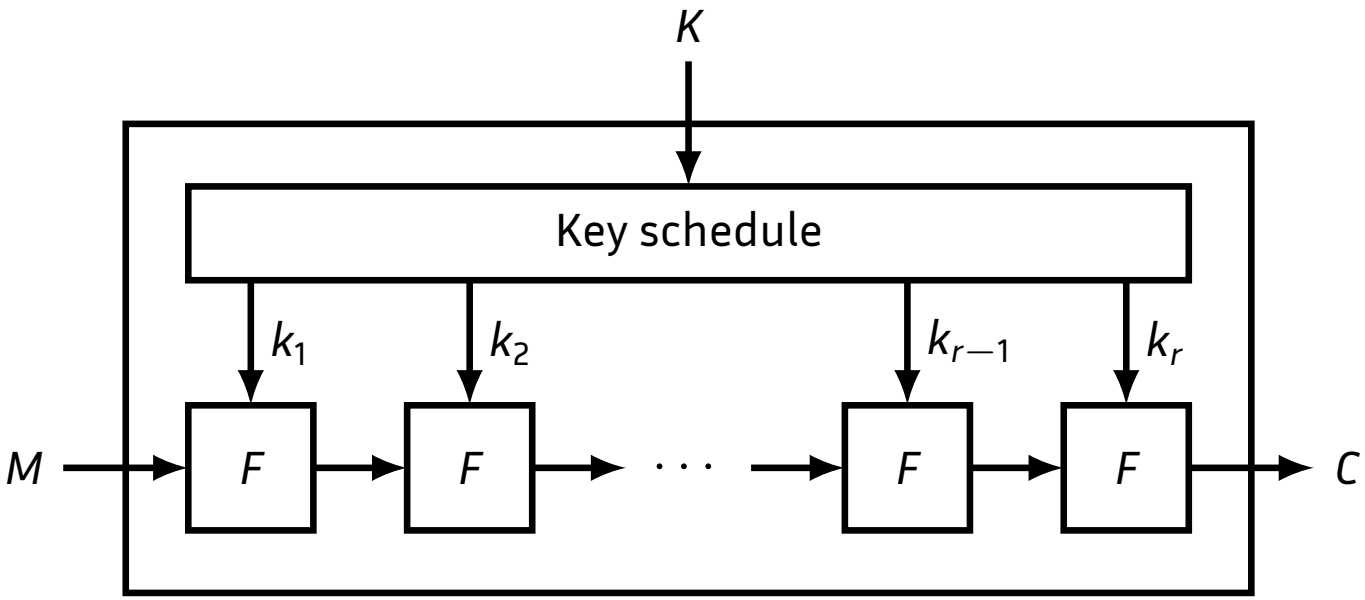
- Block ciphers

Stream ciphers vs Block ciphers

- Additive stream ciphers



- Block ciphers



Results

Block ciphers:

- Proving Resistance against Invariant attacks, CRYPTO 2017, with C. Beierle, A. Canteaut and G. Leander.

Stream ciphers and PRNG:

- Cryptanalysis of Filter generators, FSE 2016, with A. Canteaut;
- Cryptanalysis of FLIP, CRYPTO 2016, with S. Duval and V. Lallemand;
- Design of Restricted Boolean functions, ToSC 2017, with C. Carlet and P. Méaux;
- Cryptanalysis of Goldreich's PRG, ASIACRYPT 2018, with G. Couteau, A. Dupin, P. Méaux and M. Rossi.

Authenticated Encryption:

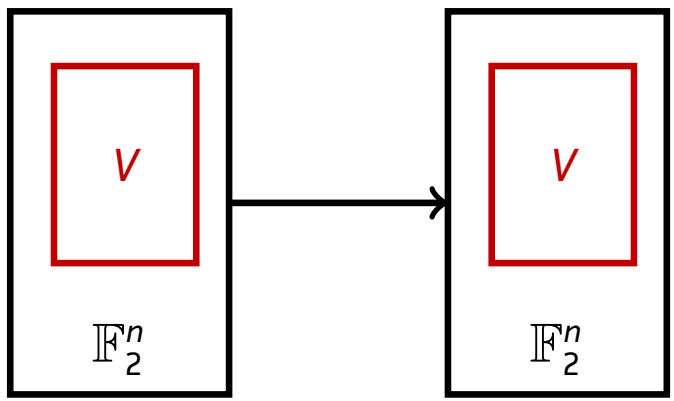
- Cryptanalysis of Ketje, ToSC 2018, with T. Fuhr and M. Naya-Pasencia;
- Cryptanalysis of MORUS, ASIACRYPT 2018, with T. Ashur, M. Eichlseder, M. M. Lauridsen, G. Leurent, B. Minaud, Y. Sasaki and B. Viguier.

Structure of this Talk

Plan of this Section

The invariant subspace attack [Leander et al. 11]

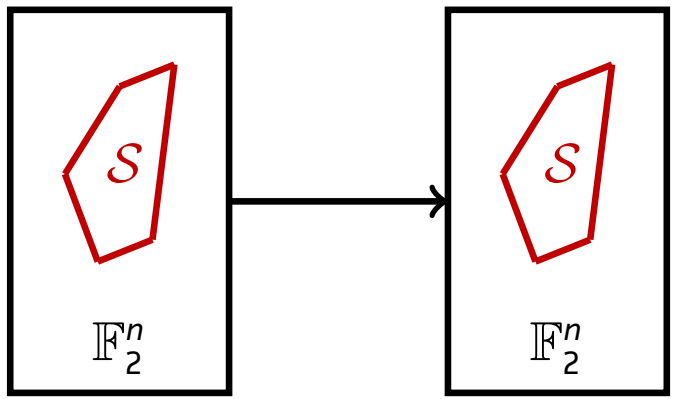
Affine subspace V invariant under E_k.



$$E_k(V) = V$$

The nonlinear invariant attack [Todo, Leander, Sasaki 16]

Partition of $\mathbb{F}_2^n$ invariant under E_k.



$$E_k(\mathcal{S}) = \mathcal{S} \text{ or } E_k(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$$

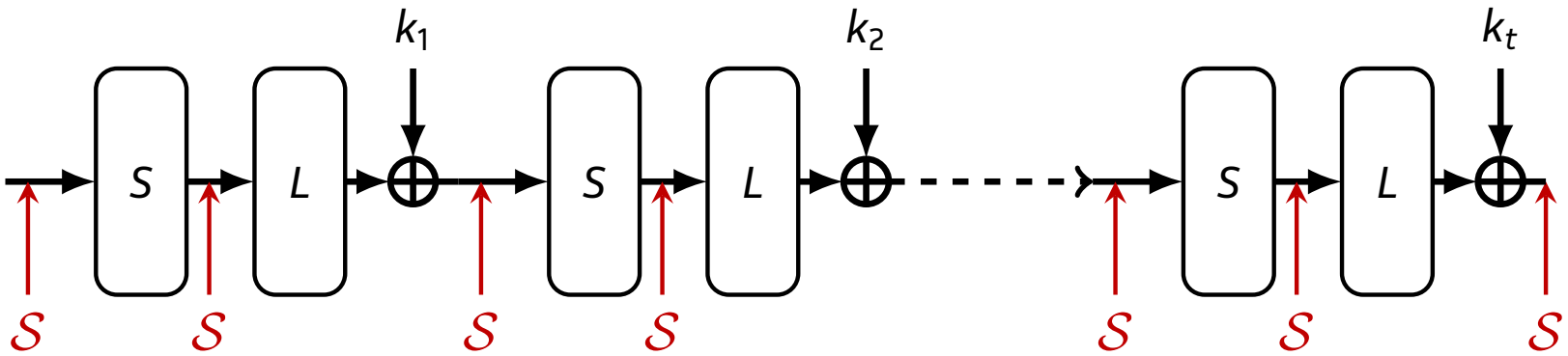
Definition (Invariant)

Let g a Boolean function such that $g(x) = 1$ iff $x \in \mathcal{S}$, then

$$\forall x \in \mathbb{F}_2^n, g \circ E_k(x) + g(x) = c \text{ with } c = 0 \text{ or } c = 1$$

g is called an **invariant for E_k**.

The case of SPN ciphers



Definition (linear structure)

$$\mathbf{LS}(g) = \{\alpha \in \mathbb{F}_2^n : x \mapsto g(x+\alpha) + g(x) \text{ is constant}\}$$

Two conditions on g

- $(k_i + k_j)$ has to be a linear structure of g.
- $\mathbf{LS}(g)$ is invariant under L.

Simple key schedule

If $k_i = k + \mathrm{RC}_i$,

$$\text{Let } D = \{(\mathrm{RC}_i + \mathrm{RC}_j)\} \text{ and}$$

$$W_L(D) = \text{smallest subspace invariant under } L \text{ which contains } D.$$

Question

Is there a non-trivial invariant g for the Sbox-layer such that

$$W_L(D) \subseteq \mathrm{LS}(g)\,?$$

The simple case

If $\dim W_L(D) \geq n - 1$, then the invariant attack does not apply.

Some lightweight block ciphers with $n = 64$:

- Skinny-64. $\dim W_L(D) = 64$ ✓
- Prince. $\dim W_L(D) = 56$ ✓ + other techniques
- Mantis-7. $\dim W_L(D) = 42$ ✓ + other techniques
- Midori-64. $\dim W_L(D) = 16$ ✗

Maximizing the dimension of $W_L(c)$

$$W_L(c) = \langle L^t(c), t \in \mathbb{N} \rangle$$

$\dim W_L(c) =$ smallest d such that there exist $\lambda_0, \ldots, \lambda_d \in \mathbb{F}_2$:

$$\sum_{t=0}^{d} \lambda_t L^t(c) = 0$$

$\dim W_L(c)$ is the degree of the minimal polynomial of c with respect to L

Theorem

There exists c such that $\dim W_L(c) = d$ if and only if d is the degree of a divisor of the minimal polynomial of L.

$$\max_{c \in \mathbb{F}_2^n} \dim W_L(c) = \deg \mathrm{Min}_L$$

Examples

- **LED.** $\mathrm{Min}_L = (X^8 + X^7 + X^5 + X^3 + 1)^4 (X^8 + X^7 + X^6 + X^5 + X^2 + 1)^4$ then there exist some c such that $\dim W_L(c) = 64$
- **Skinny-64.** $\mathrm{Min}_L = X^{16} + 1 = (X + 1)^{16}$ then there exist some c such that $\dim W_L(c) = d$ for any $1 \leq d \leq 16$
- **Prince.** $\mathrm{Min}_L = (X^4 + X^3 + X^2 + X + 1)^2 (X^2 + X + 1)^4 (X + 1)^4$ $\max_c \dim W_L(c) = 20$
- **Mantis and Midori.** $\mathrm{Min}_L = (X + 1)^6$ $\max_c \dim W_L(c) = 6$

Rational canonical form

- When $\deg(\mathrm{Min}_L) = n$, L is similar to the companion matrix:

$$C(\mathrm{Min}_L) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ p_0 & p_1 & p_2 & \dots & p_{n-1} \end{pmatrix}$$

- More generally,

$$\begin{pmatrix} C(Q_1) & & & \\ & C(Q_2) & & \\ & & \ddots & \\ & & & C(Q_r) \end{pmatrix}$$

$Q_1 = \mathrm{Min}_L, Q_2, \dots, Q_r$ are the invariant factors of L, with $Q_i \mid Q_{i-1}$ for all $1 \leq i \leq r$.

Example

For Prince.

$$\begin{aligned}\mathrm{Min}_L(X) &= X^{20}+X^{18}+X^{16}+X^{14}+X^{12}+X^8+X^6+X^4+X^2+1\\ &= (X^4+X^3+X^2+X+1)^2(X^2+X+1)^4(X+1)^4\end{aligned}$$

8 invariant factors:

$$\begin{aligned}Q_1(X) &= Q_2(X)\\ &= X^{20}+X^{18}+X^{16}+X^{14}+X^{12}+X^8+X^6+X^4+X^2+1\\ Q_3(X) &= Q_4(X) = X^8+X^6+X^2+1 = (X+1)^4(X^2+X+1)^2\\ Q_5(X) &= Q_6(X) = Q_7(X) = Q_8(X) = (X+1)^2\end{aligned}$$

Maximizing the dimension of $W_L(c_1, \ldots, c_t)$

Theorem

Let $Q_1, Q_2, \ldots, Q_r$ be the r invariant factors of L. For any $t \leq r$,

$$\max_{c_1,\ldots,c_t} \dim W_L(c_1, \ldots, c_t) = \sum_{i=1}^{t} \deg Q_i.$$

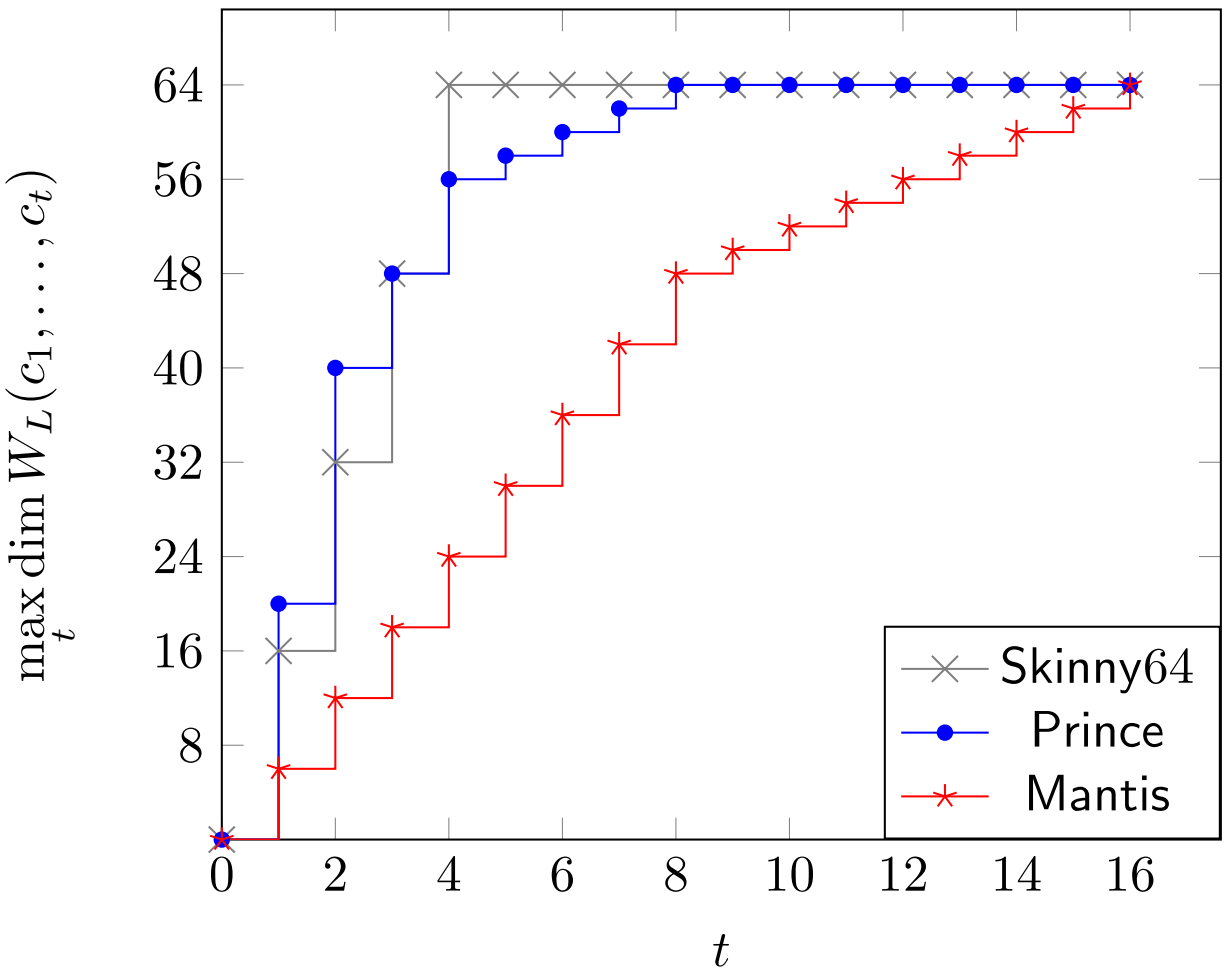
We need r elements to get $W_L(D) = \mathbb{F}_2^n$.

For Prince.

$$\text{For } t = 5, \ \max \dim W_L(c_1, \ldots, c_5) = 20 + 20 + 8 + 8 + 2 = 58$$

We need **8** elements to get the full space.

Maximum dimension for #D constants



For random constants

For $t \geq r$,

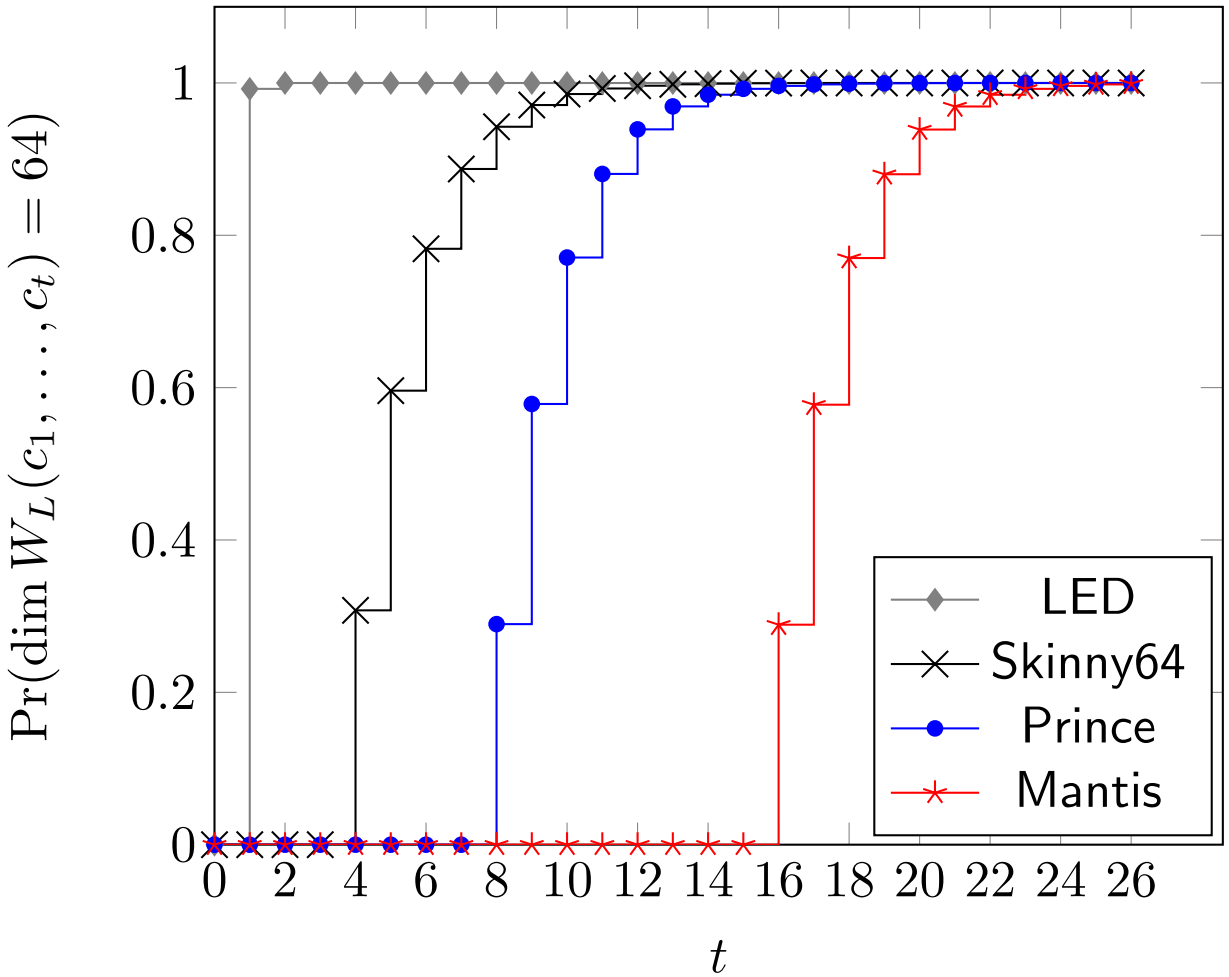
$$\Pr_{c_1,\ldots,c_t \xleftarrow{\$} \mathbb{F}_2^n} [W_L(c_1, \cdots, c_t) = \mathbb{F}_2^n]$$

can be computed from the degrees of the irreducible factors of $\mathbf{Min}_L$ and from the invariant factors of L.

LED: $\mathrm{Min}_L(X) = (X^8 + X^7 + X^5 + X^3 + 1)^4 (X^8 + X^7 + X^6 + X^5 + X^2 + 1)^4$

$$\Pr_{c \xleftarrow{\$} \mathbb{F}_2^{64}} [W_L(c) = \mathbb{F}_2^{64}] = (1 - 2^{-8})^2 \simeq 0.9922$$

Probability to achieve the full dimension



Conclusion

Easy to prevent the attack:

- by choosing a linear layer which has a few invariant factors
- by choosing appropriate round constants

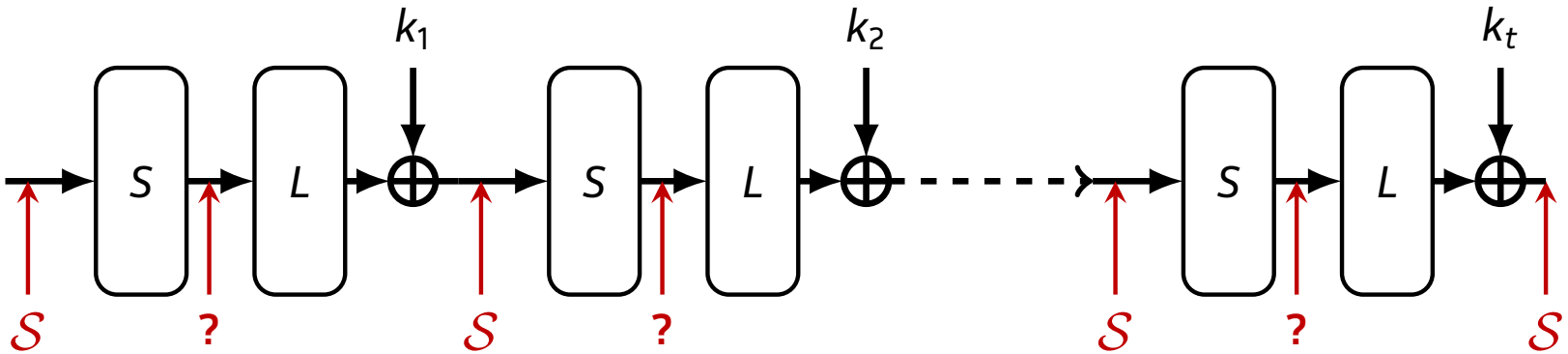
Perspectives: Use different invariants for the Sbox-layer and the linear layer?

Conclusion

Easy to prevent the attack:

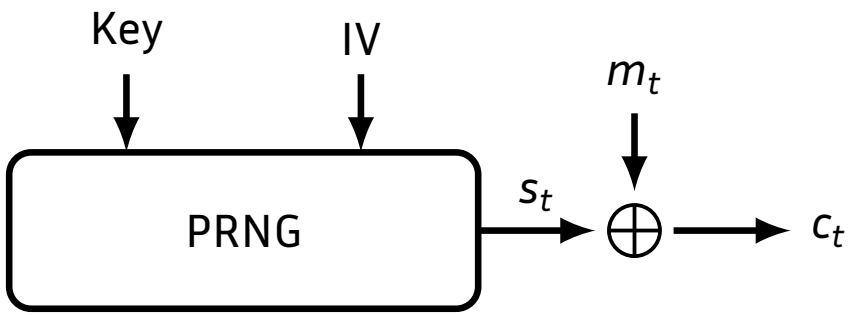
- by choosing a linear layer which has a few invariant factors
- by choosing appropriate round constants

Perspectives: Use different invariants for the Sbox-layer and the linear layer?



Plan of this Section

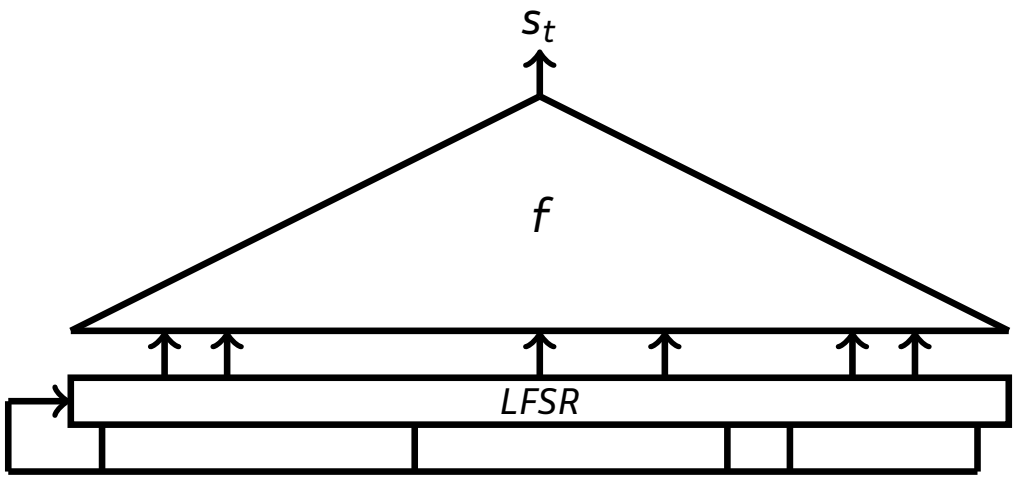
Stream ciphers



Filtered LFSR

P : the (primitive) characteristic polynomial of the LFSR.

f : nonlinear filtering function.



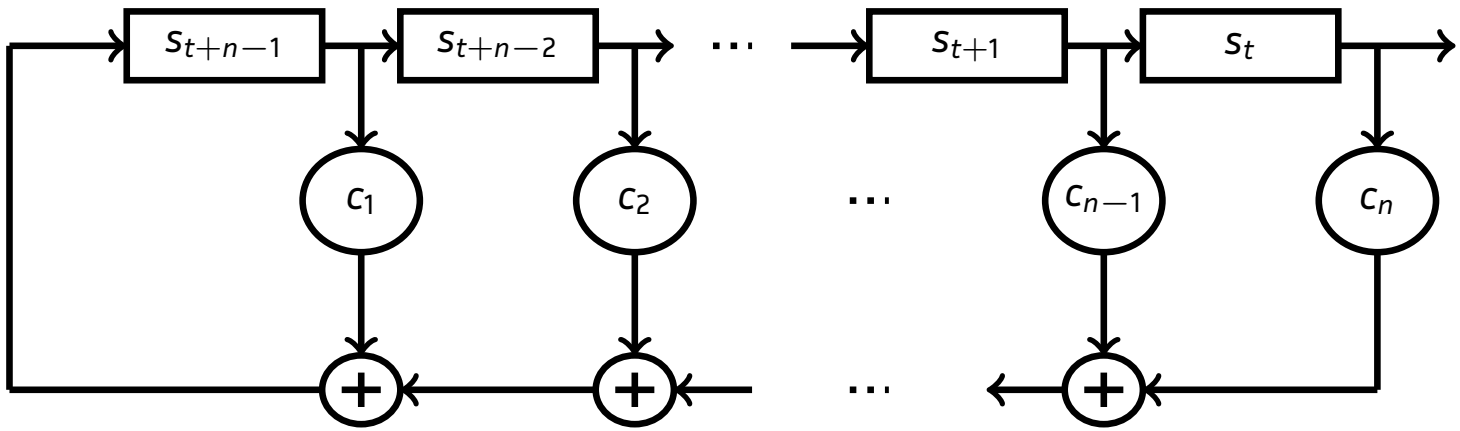
Algebraic Normal Form

$$f(x_1, x_2, \cdots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i}$$

$$= a_0 + a_1 x_1 + a_2 x_2 + \cdots + a_3 x_1 x_2 + \cdots + a_{2^n-1} x_1 \cdots x_n$$

Finite Field Representation of an LFSR

- α : root of the primitive characteristic polynomial in $\mathbb{F}_{2^n}$
- Identify the n-bit words with elements of $\mathbb{F}_{2^n}$ with the dual basis of $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$

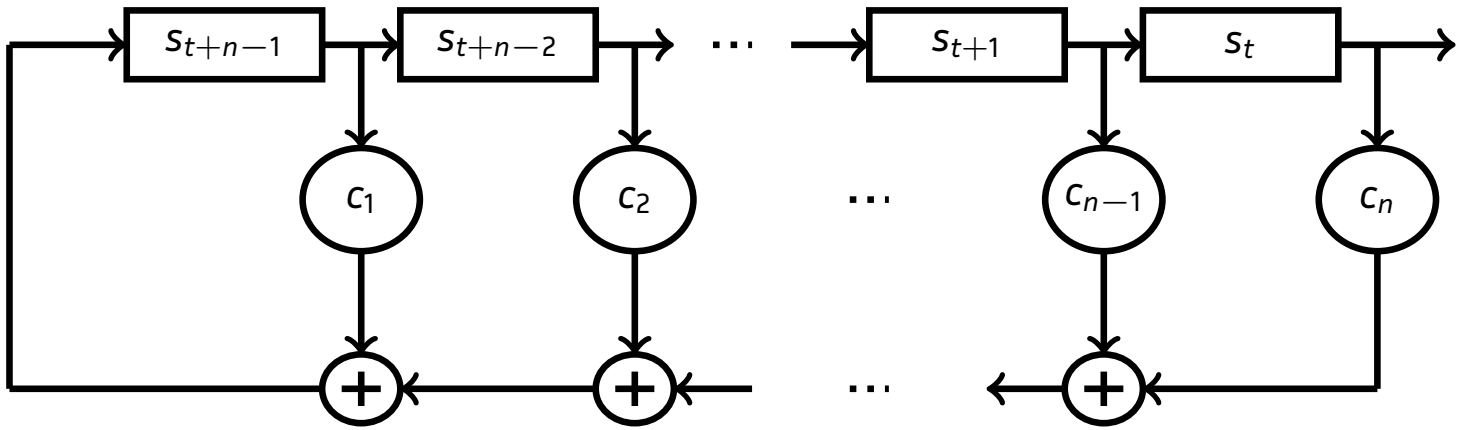


Proposition

The state of the LFSR at time $(t+1)$ is the state of the LFSR at time t multiplied by α.

Finite Field Representation of an LFSR

- α : root of the primitive characteristic polynomial in $\mathbb{F}_{2^n}$
- Identify the n-bit words with elements of $\mathbb{F}_{2^n}$ with the dual basis of $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$



Proposition

The state of the LFSR at time $(t+1)$ is the state of the LFSR at time t multiplied by α.

For all t, $X_t = X_0 \alpha^t$

Boolean functions

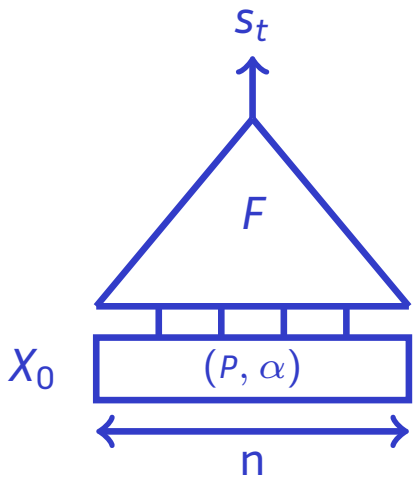
Proposition (Univariate representation)

$$F(X) = \sum_{i=0}^{2^n-1} A_i X^i$$

with $A_i \in \mathbb{F}_{2^n}$ given by the Discrete Fourier Transform of F

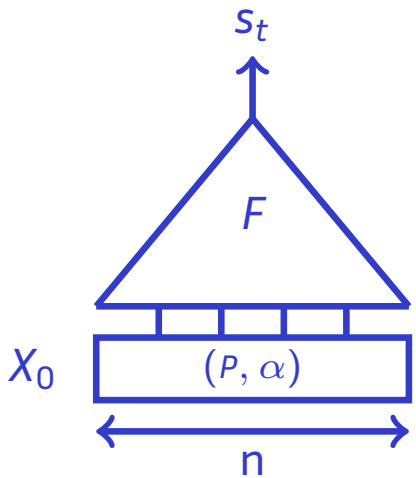
For all t, $s_t = F(X_0 \alpha^t)$

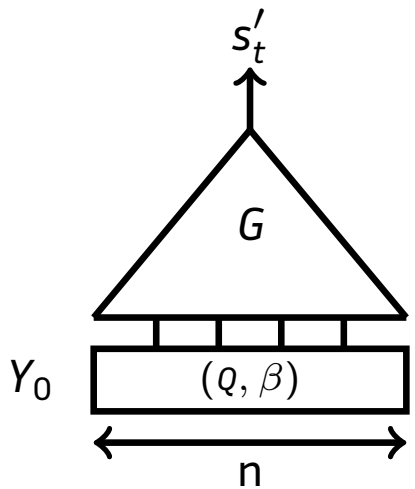
Monomial equivalence [Rønjom, Cid 10]



For all t, $s_t = F(X_0 \alpha^t)$

Monomial equivalence [Rønjom, Cid 10]

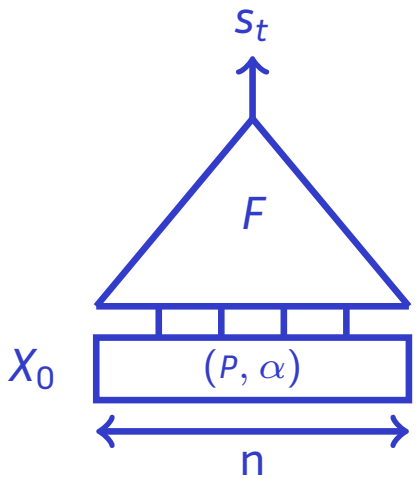


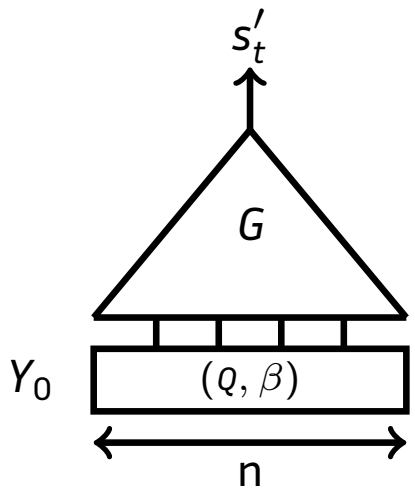


For all t, $s_t = F(X_0\alpha^t)$

$$\beta = \alpha^k \text{ with } \gcd(k, 2^n - 1) = 1$$

Monomial equivalence [Rønjom, Cid 10]

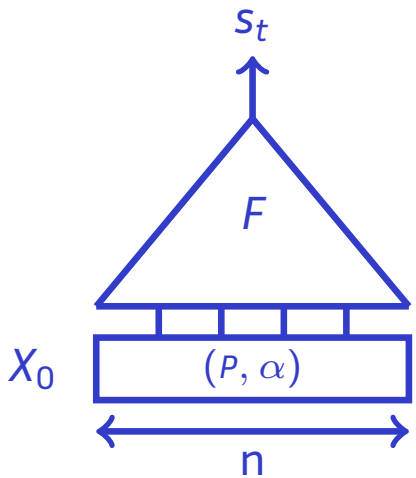


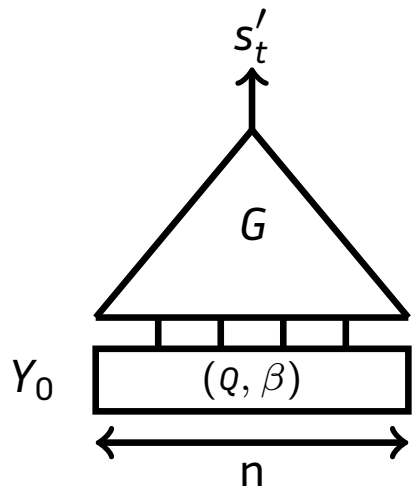


For all t, $s_t = F(X_0\alpha^t)$

$$\beta = \alpha^k \text{ with } \gcd(k, 2^n - 1) = 1$$
$$s'_t = G(Y_0\beta^t) = G(Y_0\alpha^{kt})$$

Monomial equivalence [Rønjom, Cid 10]

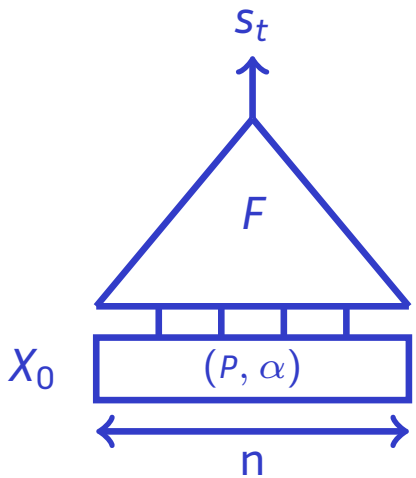


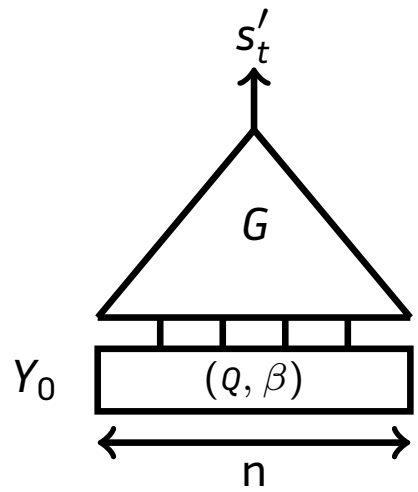


For all t, $s_t = F(X_0\alpha^t)$

$$\beta = \alpha^k \text{ with } \gcd(k, 2^n - 1) = 1$$
$$s'_t = G(Y_0\beta^t) = G(Y_0\alpha^{kt})$$
If $G(x) = F(x^r)$
with $rk \equiv 1 \mod (2^n - 1)$
Then $s'_t = F(Y_0^r\alpha^t)$

Monomial equivalence [Rønjom, Cid 10]





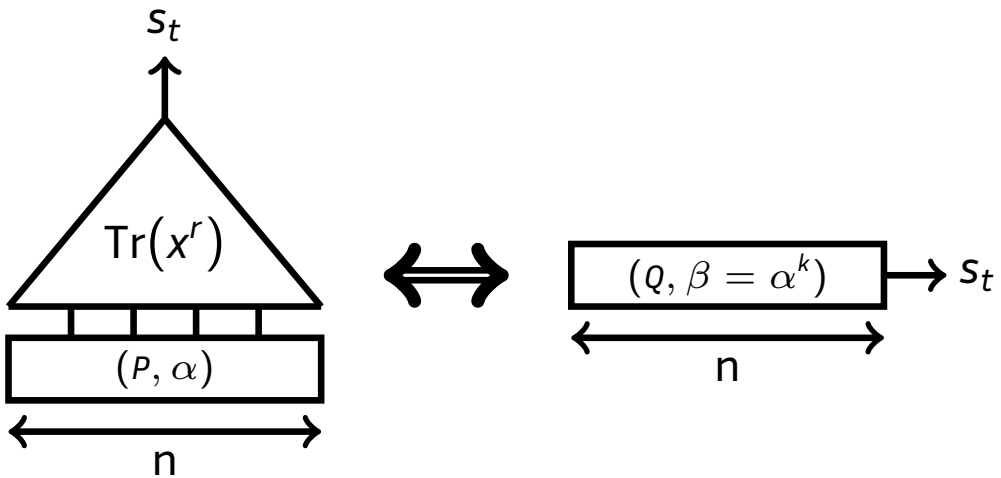
For all t, $s_t = F(X_0\alpha^t)$

$$\beta = \alpha^k \text{ with } \gcd(k, 2^n - 1) = 1$$
$$s'_t = G(Y_0\beta^t) = G(Y_0\alpha^{kt})$$
If $G(x) = F(x^r)$
with $rk \equiv 1 \mod (2^n - 1)$
Then $s'_t = F(Y_0^r\alpha^t)$

For all t, $s'_t = s_t$ **if** $Y_0 = X_0^k$

Example

$F(x) = \mathrm{Tr}(x^r)$, with $\gcd(r, 2^n - 1) = 1$:
Let k be such that $rk \equiv 1 \mod (2^n - 1)$.



$\Longrightarrow$ The initial generator is equivalent to a plain LFSR of the same size.

Consequence

The security level of a filtered LFSR is the minimal security level for a generator of its equivalence class.

- Algebraic attacks
- Correlation attacks

Algebraic attacks

Λ : Linear complexity

Proposition (Massey-Serconek 94)

Consider an LFSR of size n filtered by a Boolean function F:

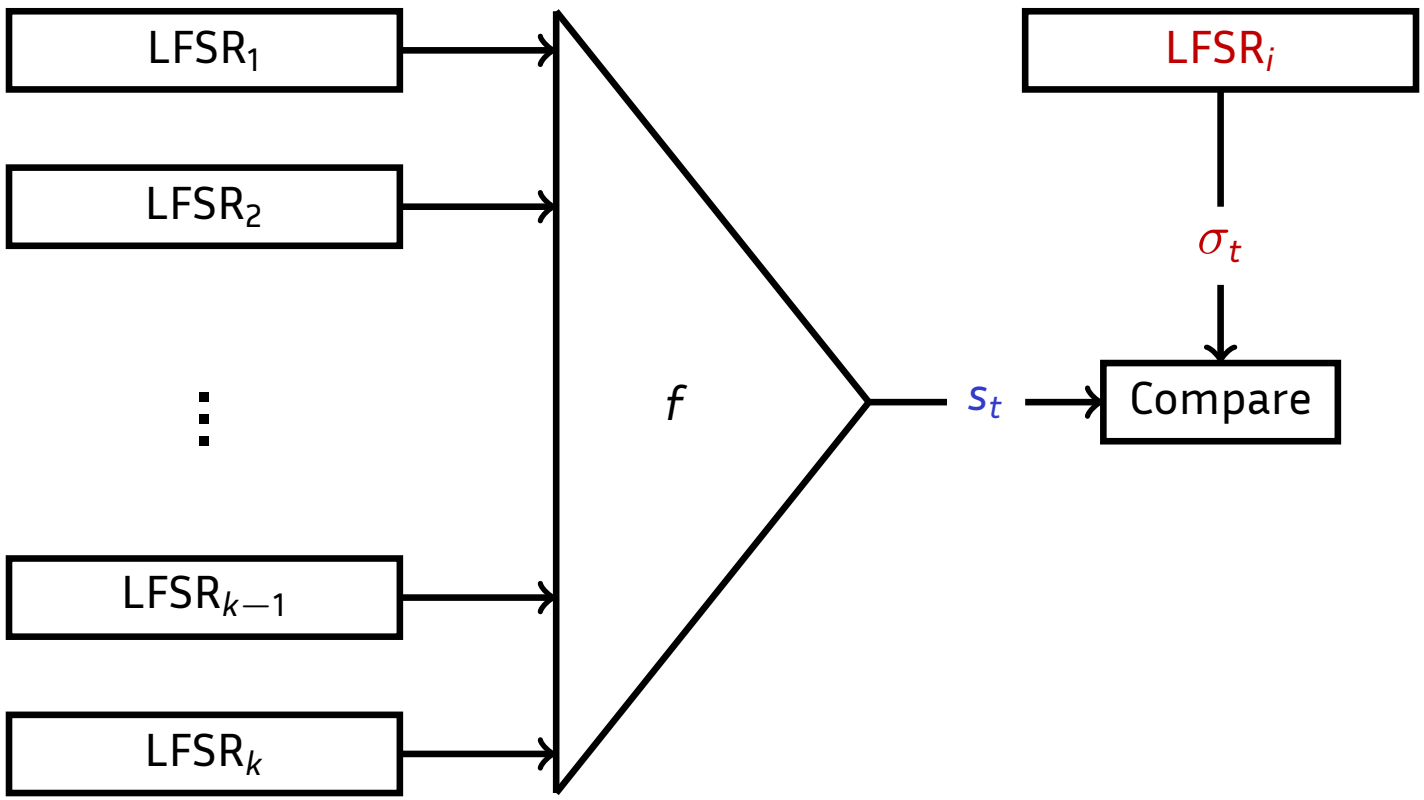
$$F(X) = \sum_{i=0}^{2^n-1} A_i X^i$$

Then

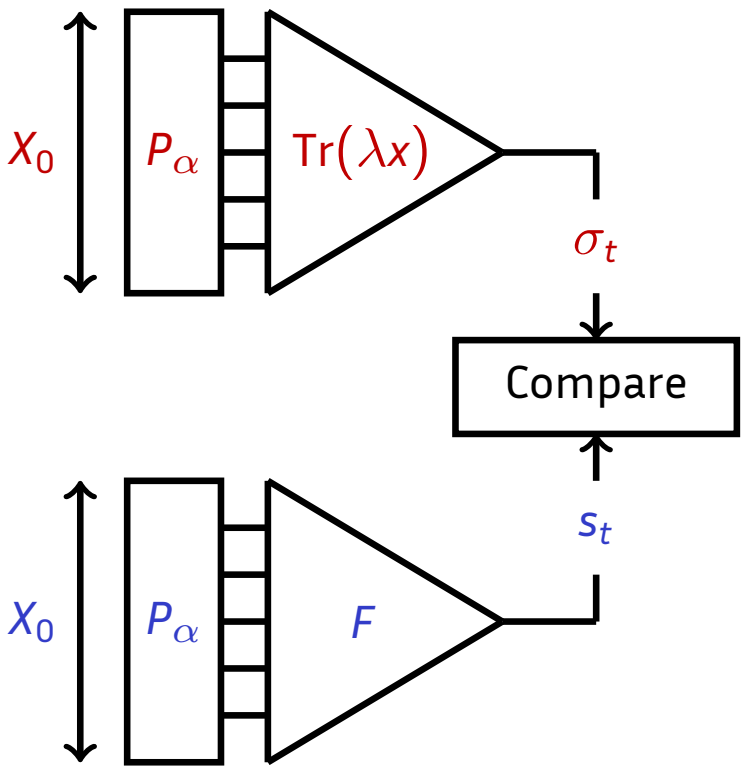
$$\Lambda = \#\{0 \leq i \leq 2^n - 2 : A_i \neq 0\}$$

The monomial equivalence does not affect the complexity of algebraic attacks [Gong et al. 11]

Correlation attack [Siegenthaler 85]

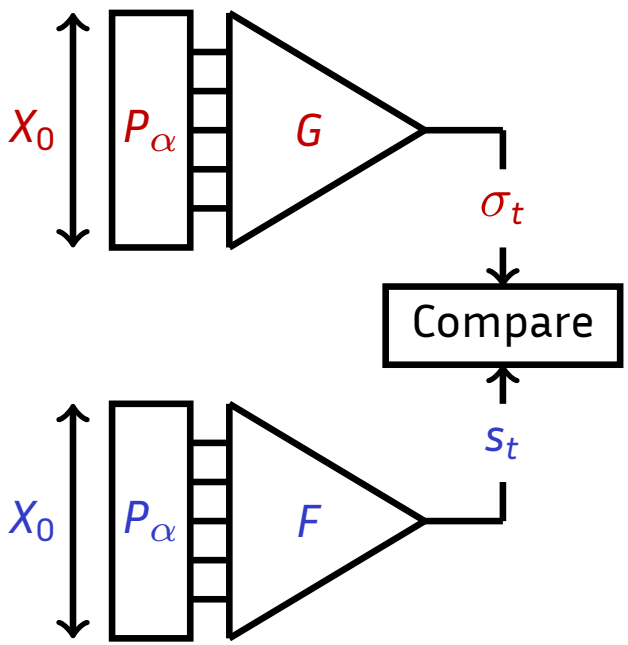


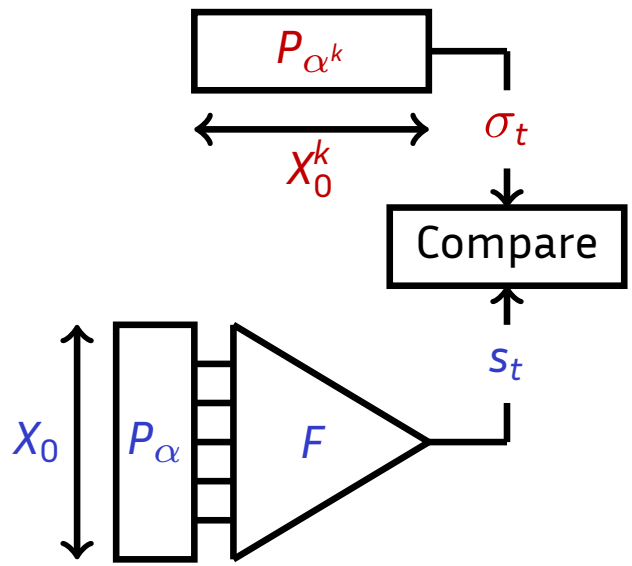
Fast correlation attack [Meier, Staffelbach 88]



Generalized fast correlation attacks

$$G(x) = \mathrm{Tr}(\lambda x^k)$$





Generalized non-linearity [Gong, Youssef 01]

Relevant security criterion:

Generalized non-linearity

$$\mathsf{GNL}(f) = d\left(f, \left\{\mathsf{Tr}\left(\lambda x^{k}\right), \lambda \in \mathbb{F}_{2^n}, \gcd\left(k, 2^n - 1\right) = 1\right\}\right)$$

Generalized non-linearity [Gong, Youssef 01]

Relevant security criterion:

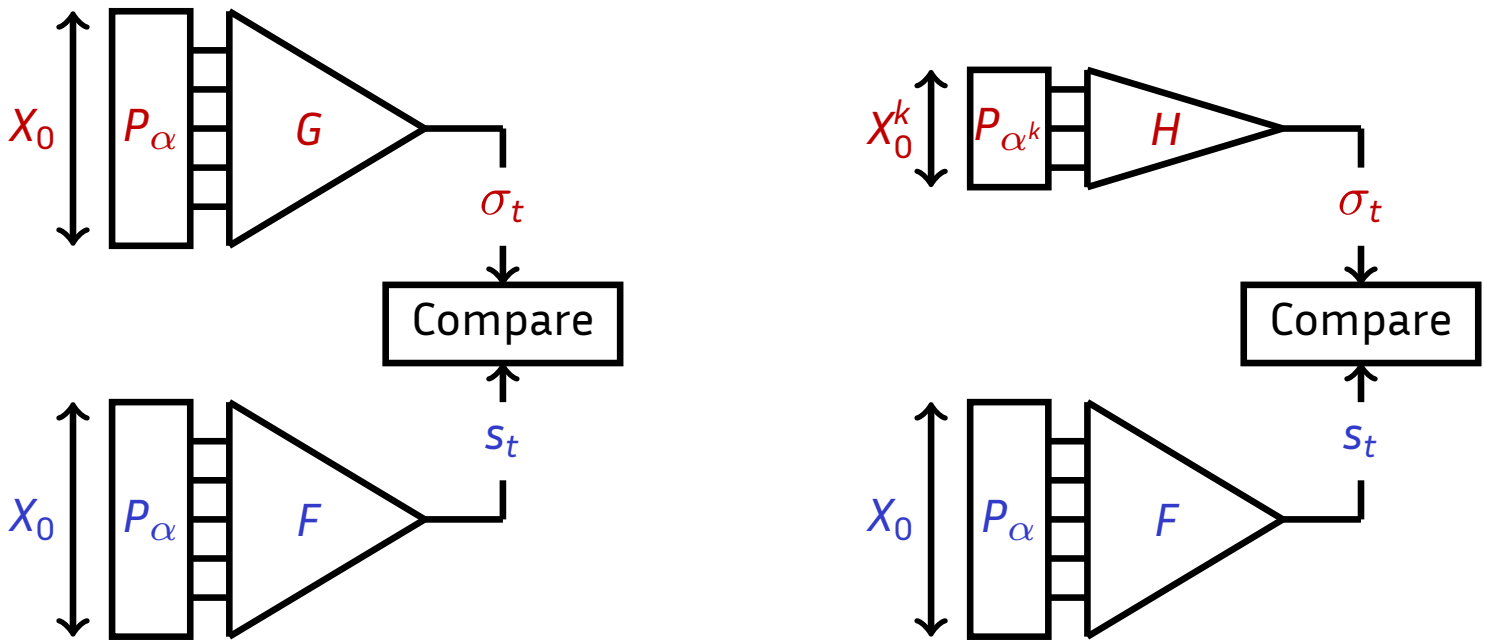
Generalized non-linearity

$$\mathsf{GNL}(f) = d\left(f, \left\{\mathsf{Tr}\left(\lambda x^{k}\right), \lambda \in \mathbb{F}_{2^n}, \gcd\left(k, 2^n - 1\right) = 1\right\}\right)$$

And if k is not coprime to $2^n - 1$?

A more efficient correlation attack

When $\gcd(k, 2^n - 1) > 1$ and F correlated to $G(X) = H(X^k)$.



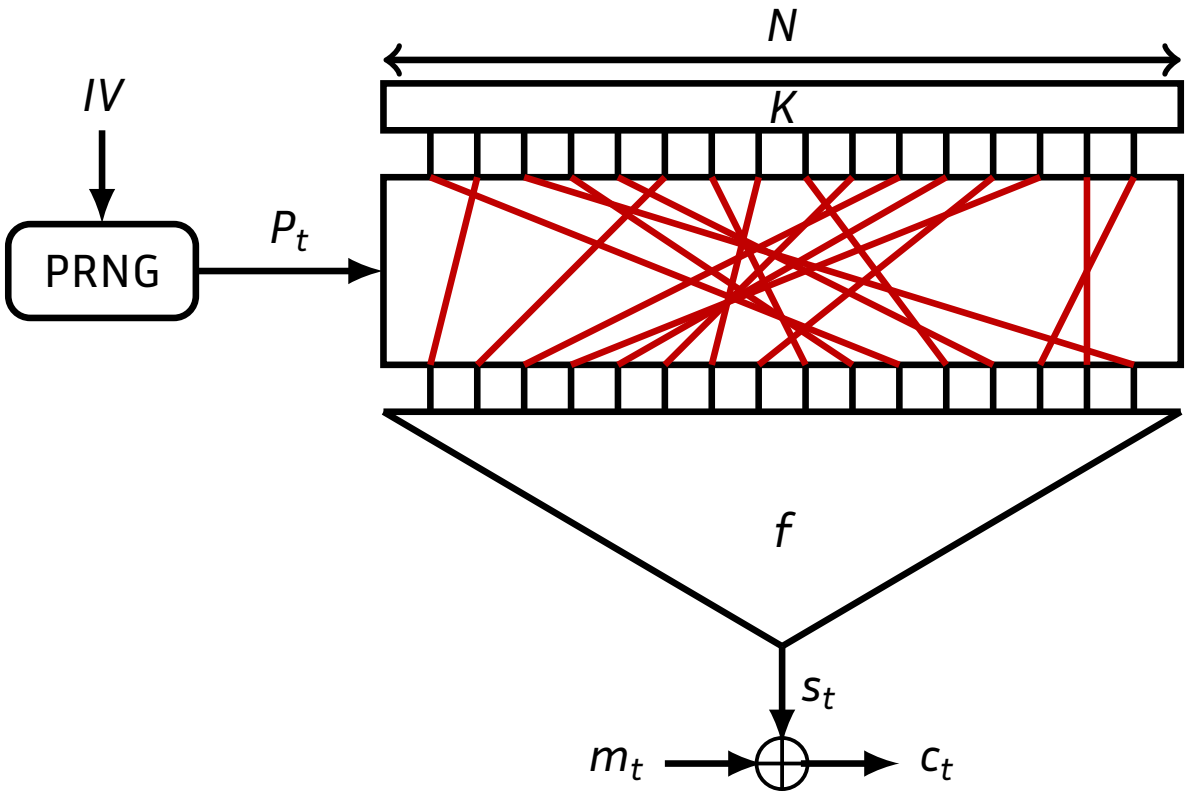
- Number of states of the small generator: $\tau_k = \mathrm{ord}(\alpha^k)$.
- Exhaustive search on X_0^k: Time $= \frac{\tau_k \log(\tau_k)}{\varepsilon^2}$
- Improvement with an FFT [Canteaut - Naya-Plasencia, 2012]:
  Time $= \tau_k \log \tau_k + \frac{2 \log(\tau_k)}{\varepsilon^2}$

Implications

- Decomposition in multiplicative subgroups of $\mathbb{F}_{2^n}^*$.
- Divide-and-conquer technique.
- The attack does not apply when $(2^n - 1)$ is prime.

Plan of this Section

FLIP [Méaux et al. 16]



- Constant Key Register: size N
- Filtering function F

Preliminary version of FLIP

FLIP	n	degree	Key size (N)	Security
FLIP-80	12	14	192	80
FLIP-128	19	21	400	128

$$f(x_0, \cdots, x_{191}) = x_0 + \ldots + x_{46} + x_{47}x_{48} + \ldots + x_{85}x_{86} + x_{87} + x_{88}x_{89}$$
$$+x_{90}x_{91}x_{92} + x_{93}x_{94}x_{95}x_{96} + x_{97}x_{98}x_{99}x_{100}x_{101} + \ldots + x_{178}x_{179}\cdots x_{190}x_{191}$$

Cryptanalysis

Classical attacks

- Algebraic Immunity
- Non Linearity
- Resiliency

Cryptanalysis

Classical attacks

- Algebraic Immunity
- Non Linearity
- Resiliency

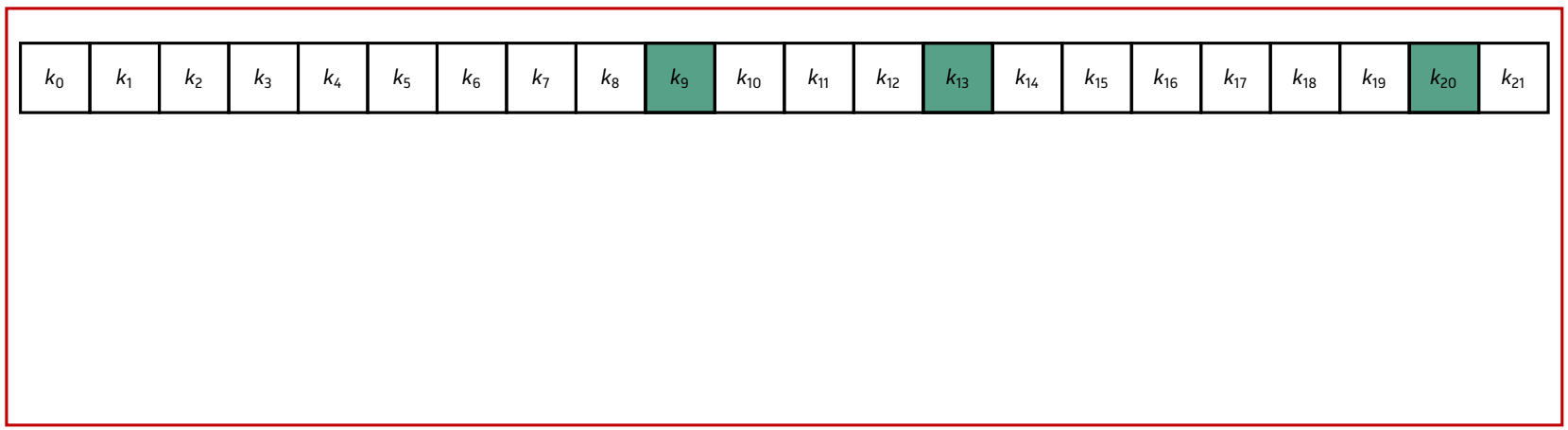
Our attack

- Use a Guess-and-determine technique to have a simpler function
- Combine with a classical attack on the reduced Boolean function

Our attack

1. Guess ℓ random positions of 0 bits
2. Keep an equation when there is at least **one** 0 bit in each monomial of degree at least 3
3. Solve the system of degree 2

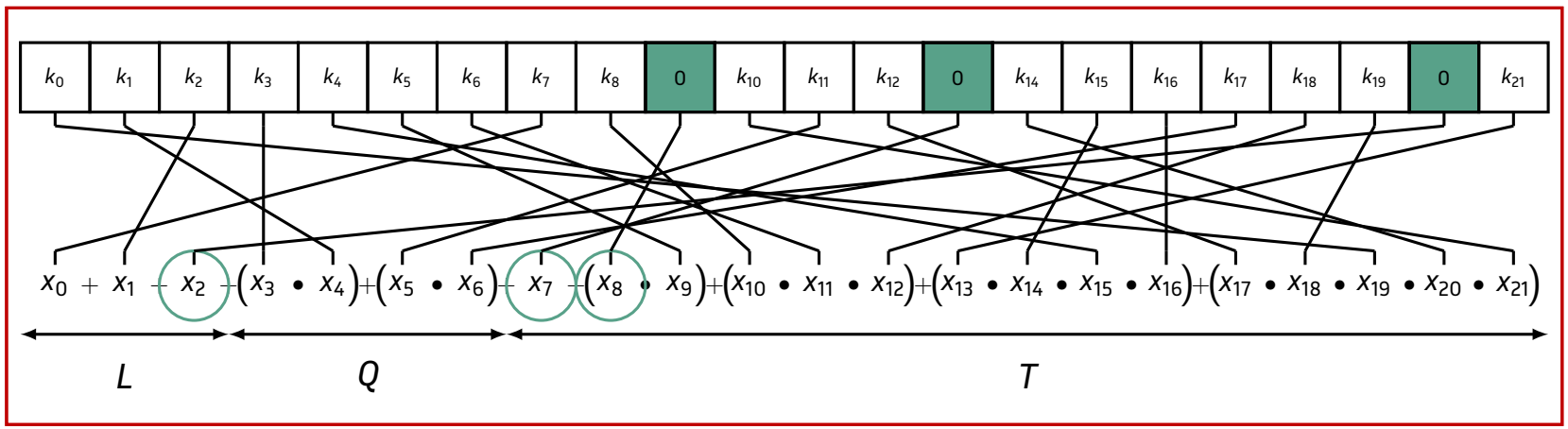
Get equations of degree ≤ 2



Get equations of degree ≤ 2

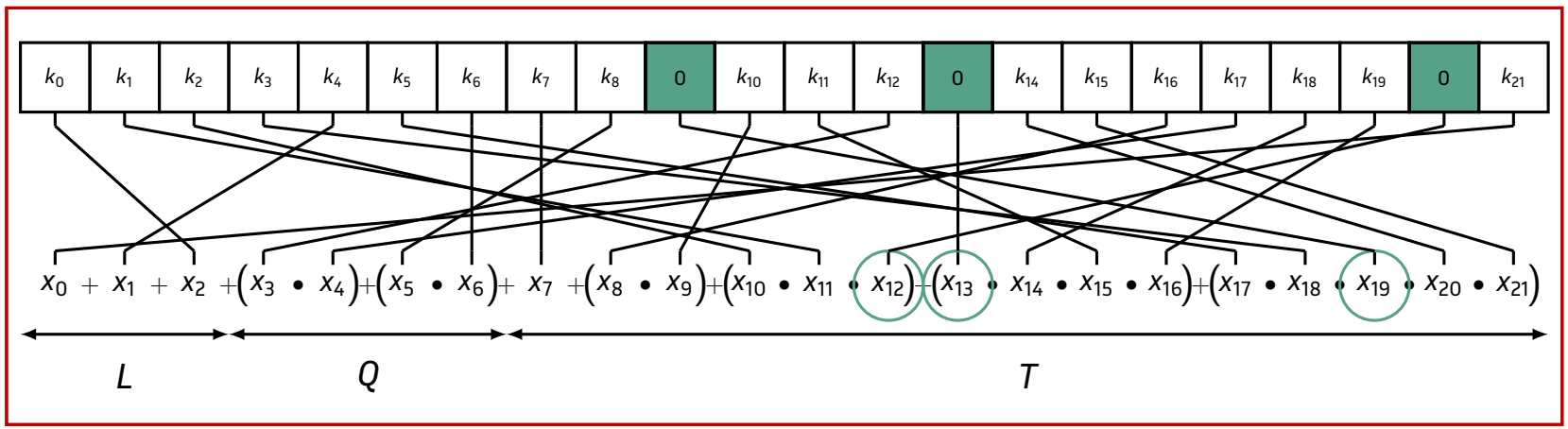
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	0	k_{10}	k_{11}	k_{12}	0	k_{14}	k_{15}	k_{16}	k_{17}	k_{18}	k_{19}	0	k_{21}

Get equations of degree ≤ 2



$$s_t = k_7 + k_2 + k_3k_1 + k_{11}k_{17} + 0 + 0 + k_8k_6k_{18} + k_{21}k_{15} + k_{21}k_{15}k_4k_{16} + k_{12}k_{19}k_0k_{14}k_{10}$$

Get equations of degree ≤ 2



$$s_{t+1} = k_{21} + k_4 + k_0 + k_{12}k_{17} + k_8k_6 + k_7 + k_{16}k_{10}$$

Complexity

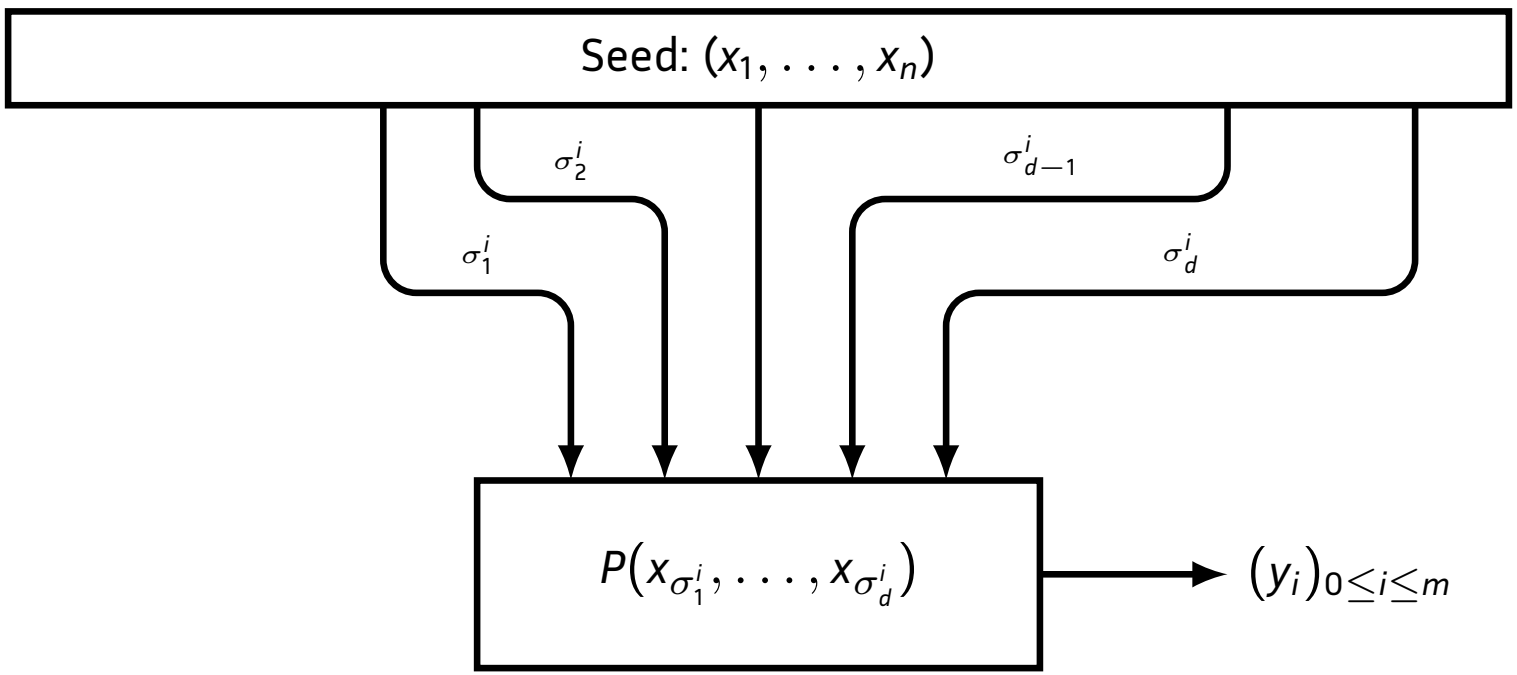
80-bit security claim :

$$C_T = 2^{54.5}, C_D = 2^{40.3}, C_M = 2^{28.0}$$

128-bit security claim :

$$C_T = 2^{68.1}, C_D = 2^{58.5}, C_M = 2^{32.3}$$

Goldreich's PRG [Goldreich 00]



$$P_5(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 + x_4 x_5$$

Plan of this Section

Conclusion

- Properties of Buildings Blocks are important.
- Relevance depends on contexts and cryptanalysis.

Perspectives

Multivariate	Univariate
Algebraic Immunity	Spectral Immunity
Resiliency	
Non-linearity	

Perspectives

Multivariate	Univariate
Algebraic Immunity	Spectral Immunity
Resiliency	Subgroup resiliency
Non-linearity	Generalized Non-linearity

Perspectives

Multivariate	Univariate
Algebraic Immunity	Spectral Immunity
Resiliency	Subgroup resiliency
Non-linearity	Generalized Non-linearity

- Link between representations? Between criteria?

Perspectives

Multivariate	Univariate
Algebraic Immunity	Spectral Immunity
Resiliency	Subgroup resiliency
Non-linearity	Generalized Non-linearity

- Link between representations? Between criteria?
- Find new representations?